IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method carried out by a computer when executing computer-readable program code, the method comprising:

receiving a certain electronic file intended for delivery from a sender to an intended recipient, the certain electronic file having a first file format having a first file extension and containing a computer virus; and

prior to the certain electronic file being made available for viewing by the intended recipient, converting the certain electronic file to a second file format having a second file extension that is different from the first file extension of the first file format and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient;

wherein it is determined whether the certain electronic file represents at least a potential risk to security of a computer system, said converting the certain electronic file being in response to a determination that the certain electronic file represents at least the potential risk to the security of the computer system.

2. (Original) The method of claim 1, the certain electronic file being an attachment to an electronic mail sent over a network.

3. (Original) The method of claim 2, the network including the internet.

4. (Original) The method of claim 1, said receiving occurring at a desktop computer of the intended recipient.

5. (Original) The method of claim 1, said receiving occurring at a server computer.

6. (Original) The method of claim 1, said receiving occurring at a gateway computer.

7. (Original) The method of claim 1, said converting occurring at a desktop computer of the intended recipient.

8. (Original) The method of claim 1, said converting occurring at a server computer.

9. (Original) The method of claim 1, said converting occurring at a gateway computer.

10. (Original) The method of claim 1, said converting occurring prior to the intended recipient receiving the certain electronic file.

11. (Cancelled)

12 (Previously Amended) The method of claim 1, said determining whether the certain electronic file represents the potential risk comprising:

determining if the certain electronic file contains the computer virus.

13. (Previously Amended) The method of claim 1, said determining whether the certain electronic file represents the potential risk comprising:

conducting a heuristic scan of the certain electronic file.

14. (Original) The method of claim 1, the certain electronic file being a first electronic file, further comprising:

receiving a second electronic file intended for delivery from another sender to another intended recipient, the second electronic file having a third file format and containing another computer virus; and

prior to the second electronic file being made available for viewing by the another intended recipient, converting the second electronic file to a fourth file format that is

different from the third file format and that prevents the another computer virus from executing when the converted second electronic file is opened by the another intended recipient.

15. (Original) The method of claim 1, the computer virus including a macro virus.

16. (Original) The method of claim 1, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format.

17. (Original) The method of claim 16, the second file format being the HTML file format without scripts.

18. (Original) The method of claim 16, the second file format being the ACSII file format file.

19. (Original) The method of claim 16, the second file format being the TXT file format.

20. (Original) The method of claim 1, the second file format being a file format having text without scripts.

21. (Original) The method of claim 1, the certain electronic file being at least one of a word processing file, a spreadsheet file, a database file, a graphics file, a presentation file, a compressed file, and a binary executable file.

22. (Original) The method of claim 1, further comprising:

determining if the first file format is one of a word processing file format type and a graphics file format type, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it

is determined that the certain file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type.

23. (Original) The method of claim 1, the certain electronic file being an electronic file received by at least one of a RTP transfer or a HTTP transfer protocol.

24. (Currently Amended) A method for implementing a security policy, the method comprising:

determining whether an electronic file represents at least a potential risk to security of a computer system; and

prior to making the electronic file available to an intended recipient of the electronic file, converting the electronic file into a safe format having a safe file extension that ensures that a computer virus in the electronic file is unable to harm the computer system;

said converting the electronic file being in response to the determination that the electronic file represents at least the potential risk to the security of the computer system.

25. (Original) The method of 24, said determining comprising:

determining whether the electronic file has a file extension indicative of a file type that supports a potential computer virus.

26. (Original) The method of 24, said determining comprising:

detecting whether the electronic file contains the computer virus.

27. (Original) The method of 24, said determining comprising:

determining whether content of the electronic file reflects a potential computer virus.

28. (Currently amended) A computer-readable medium having instructions stored thereon, the instructions when executed by a computer cause the computer to:

convert a certain electronic file, intended for delivery from a sender to an intended recipient, from a first file format having a first file extension to a second file format having a second file extension, said converting being prior to the certain electronic file being made available for viewing by the intended recipient, the second file format with the second file extension being different from the first file format with the first file extension and preventing a computer virus in the certain electronic file from executing when the converted electronic file is opened by the intended recipient;

wherein it is determined whether the certain electronic file represents at least a potential risk to security of a computer system, said converting the certain electronic file being in response to a determination that the certain electronic file represents at least the potential risk to the security of the computer system.

29. (Original) The computer-readable medium of claim 28, the certain electronic file being an attachment to an electronic mail sent over a network.

30. (Original) The computer-readable medium of claim 28, the instructions when executed by the computer cause the computer to convert the certain electronic file from the first file format to the second file format prior to the intended recipient receiving the certain electronic file.

31. (Cancelled)

32. (Previously Amended) The computer-readable medium of claim 28 said determining whether the certain electronic file represents the potential risk comprising:

determining if the certain electronic file contains the computer virus.

33. (Original) The computer-readable medium of claim 28, the instructions when executed by the computer further cause the computer to:

determine if the first file format is one of a word processing format type and a graphics format type, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the first file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type.

34. (Original) The computer-readable medium of claim 28, the computer virus being a macro virus.

35. (Original) The computer-readable medium of claim 28, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format.

36. (Currently Amended) An apparatus comprising:

a computer having means for receiving a certain electronic file intended for delivery from a sender to a intended recipient, the certain electronic file having a first file format having a first file extension and containing a computer virus, the computer further including means for converting, prior to the certain electronic file being made available for viewing by the intended recipient, the certain electronic file from the first file format with the first file extension to a second file format having a second file extension that is different from the first file format with the first file extension and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient;

wherein it is determined whether the certain electronic file represents at least a potential risk to security of a computer system, said converting the certain electronic file being in response to a determination that the certain electronic file represents at least the potential risk to the security of the computer system.

37. (Original) The apparatus of claim 36, said computer being a desktop computer of the intended recipient.

38. (Original) The apparatus of claim 36, said computer being a server computer of a local area network.

39. (Original) The apparatus of claim 36, said computer being a gateway computer.

40. (New) The method as recited in claim 1, wherein the first format is selected from the group consisting of: a word processing file, a spreadsheet file, a database file, a graphics file, a presentation file, a compressed file, and a binary executable file; and is converted to the second format which is selected from the group consisting of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format.